Homework 3 : Due Wednesday, February 17

Problem 1: In Theorem 14.6, Bolker shows that every odd integers is the difference of two squares. Show that an even integer is the difference of two squares if and only if it is divisible by 4.

Problem 2: Prove the converse to Wilson's Theorem: If $n \geq 2$ and $(n-1)! \equiv_n -1$, then n is prime.

Problem 3: Let p be a prime, and let $F = \mathbb{Z}/p\mathbb{Z}$. Let $f(x), g(x) \in F[x]$. Show that the following are equivalent:

- $f(a) = g(a)$ for all $a \in F$.
- $(x^p - x) \mid (f(x) - g(x))$ in $F[x]$.

Problem 4: Let R be a commutative ring. An *idempotent* of R is an element $e \in R$ such that $e^2 = e$. For example, $0, 1 \in R$ are always idempotents. In the ring $R = \mathbb{Z} \times \mathbb{Z}$, the element $(1, 0)$ is an idempotent different from $0_R = (0, 0)$ and $1_R = (1, 1)$.
a. Show that if R is an integral domain, then the only idempotents are 0 and 1.
b. Show that if $e \in R$ is an idempotent, then $1 - e$ is also an idempotent.
c. Let p be prime and $k \geq 1$. Show that the only idempotents in $\mathbb{Z}/p^k\mathbb{Z}$ are 0 and 1.
d. Show that if m is not a prime power, then there exists an idempotent in $\mathbb{Z}/m\mathbb{Z}$ other than 0 and 1. Give a formula for the number of such idempotents in terms of the prime factorization of m. *Hint:* Instead of trying to explicitly "build" idempotents, use the Chinese Remainder Theorem to piece together information from various prime powers to get information about m.

Problem 5: Bolker, Problem 11.30acdef. Part b is extremely important, but it is long and notationally obnoxious. You should do enough to convince yourself that it is true, but you need not write any of it up. Feel free to use the result of b in other parts though.